IN THE CLAIMS

Please amend the claims to read as shown below.

37. (Previously Submitted) A system to securely utilize Basic Input and Output System (BIOS) services, comprising:

an access driver to generate a service request to utilize BIOS services, the service request including a service request signature created using a private key in a cryptographic key pair; and

an interface to verify the service request signature using a public key in the cryptographic key pair to ensure the integrity of the service request.

38. (Previously Submitted) The system of Claim 37, wherein:

the access driver generates a session request to establish a session with the interface; and

the session request includes a session request signature created using a private key in a cryptographic key pair.

39. (Previously Submitted) The system of Claim 37, wherein:

the access driver generates a session request to end the session with the interface; and

the session request includes a session request signature created using a private key in a cryptographic key pair.

40. (Previously Submitted) The system of Claim 37, wherein:

the interface generates an authority certificate and send the authority certificate to the access driver after receiving a session request; and

the access driver uses information included in the authority certificate to generate subsequent session requests.

41. (Previously Submitted) The system of Claim 40, wherein the authority certificate includes a new public key.

42. (Previously Submitted) The system of Claim 40, wherein the authority certificate includes a new private key.

43. (Previously Submitted) The system of Claim 40, wherein the authority certificate includes a certificate signature.

44. (Previously Submitted) The system of Claim 37, wherein:

the interface generates an authority certificate and sends the authority certificate to the access driver after receiving the service request; and

the access driver uses information in the authority certificate to generate subsequent service requests.

45. (Previously Submitted) A method to securely invoke Basic Input and Output System (BIOS) services, comprising:

creating a service request to invoke BIOS services;

signing the service request with a service request signature generated using a private key in a cryptographic key pair; and

verifying the service request signature using a public key in the cryptographic key pair to ensure the integrity of the service request.

46. (Previously Submitted) The method of Claim 45, further comprising:

creating an authority certificate that includes a new private key and a new public key after processing the service request;

signing a subsequent service request with a service request signature generated using the new private key; and

verifying the service request signature of the subsequent service request using the new public key

47. (Previously Submitted) The method of Claim 45, further comprising:

performing a BIOS service indicated by a service operation code included in the service request

48. (Previously Submitted) The method of Claim 45, further comprising:

creating a session request to establish a session with a ROM Application Program Interface (RAPI);

signing the session request with a session request signature generated using a private key in a cryptographic key pair; and

verifying the session request signature using a public key in the cryptographic key pair to ensure the integrity of the session request.

49. (Previously Submitted) The method of Claim 48, further comprising:

creating an authority certificate that includes a new private key and a new public key after processing the session request;

signing a subsequent session request with a session request signature generated using the new private key; and

verifying the session request signature of the subsequent session request using the new public key.

50. (Previously Submitted) The method of Claim 45, further comprising:

creating a session request to end a session with a ROM Application Program Interface (RAPI);

signing the session request with a session request signature generated using a private key in a cryptographic key pair; and

verifying the session request signature using a public key in the cryptographic key pair to ensure the integrity of the session request.

51. (Previously Submitted) A computer program embodied on a computer-readable medium to securely utilize Basic Input and Output System (BIOS) services, comprising:

an access driver to generate a service request to utilize BIOS services, the service request including a service request signature created using a private key in a cryptographic key pair; and

an interface to verify the service request signature using a public key in the cryptographic key pair to ensure the integrity of the service request.

52. Cancelled.